https://doi.org/10.7840/kics.2025.50.9.1343

연합학습 참여 유도를 위한 교대 제안 협상 기반 기기정보 비공유 인센티브 메커니즘

진 수 연◆, 차 채 연*, 박 형 곤°

A Non-Disclosure Incentive Mechanism for Federated Learning Via Alternating-offers Bargaining

Suyeon Jin◆, Chaeyeon Cha*, Hyunggon Park°

요 약

본 논문에서는 연합학습(federated learning)에서 클라이언트 기기정보의 활용 없이 연합학습의 성능을 개선하는 동시에 최적으로 보상자원을 분배하는 인센티브 메커니즘(incentive mechanism)을 제안한다. 연합학습에서 클라이언트의 자체적인 성능 평가를 반영하는 효용 함수를 정의하고, 이를 기반으로 서버에게 최소 보상정보를 전송함으로써 클라이언트 로컬 모델의 손실이나 데이터셋의 크기 등의 기기정보를 드러내지 않고 클라이언트를 선택하는 방식을 제안한다. 또한 보상자원 분배지점 결정을 위해 서버와 클라이언트 간의 협상 분해 및 교대 제안 협상을 수행함으로써 클라이언트의 효용 함수 등의 기기정보를 공유하지 않는다. 실험을 통해 제안하는 인센티브 메커니즘은 연합학습의 수렴 속도 및 정확도를 개선하며, 교대 제안 협상 기반의 보상 분배를 통해 최적 자원 분배 지점인 내쉬 협상 해법(Nash bargaining solution)을 근사한다는 것을 확인하였다.

키워드 : 연합학습, 인센티브 메커니즘, 교대 제안 협상
Key Words : Federated learning, Incentive mechanism, Alternating-offers bargaining

ABSTRACT

In this paper, we propose a non-disclosure incentive mechanism for federated learning via alternating-offers bargaining which does not utilize device information of clients while improving learning performance and approximating an optimal resource allocation. By defining utility functions of clients that reflect their self estimated performances and determining minimum compensation information, clients can be selected for participation without revealing their device information such as loss of their local model or dataset size. To determine the compensation resource allocation, server and clients perform alternating-offers bargaining, which does not require sharing their utility functions. Experiment results show that the proposed incentive mechanism can speed up convergence, improve test accuracy, and induce compensation resource allocation near the Nash bargaining soution while not revealing the device information of clients.

※ 본 연구는 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원(RS-2021-II210739)과 정부(교육부)의 재원으로 한국연구재단의 지원(RS-2024-00411580)을 받아 수행되었습니다.
◆ First Author : Ewha Womans University, Department of Electronic and Electrical Engineering, suyeon.jin@ewha.ac.kr, 학생회원
° Corresponding Author : Ewha Womans University, Department of Electronic and Electrical Engineering, hyunggon.park@ewha.ac.kr, 종신회원
* Ewha Womans University, Department of Electronic and Electrical Engineering, chaeyeon.cha@ewha.ac.kr
논문번호 : 202502-038-A-RN, Received February 20, 2025; Revised April 3, 2025; Accepted April 22, 2025

Ⅰ. 서 론

최근 사물인터넷(Internet of Things) 및 클라우드 컴퓨팅(cloud computing)의 활용 범위가 넓어지면서, 분산된 다수의 디바이스(device)들에서 데이터셋이 대규모로 생성되고 있다. 이에 따라 지속적으로 생성되는 대규모 데이터셋을 이용하여 인공지능 모델을 학습시키고 개선된 서비스를 제공하는 방식에 대한 관심 또한 증가하였다[1,2]. 기존의 머신러닝(machine learning)은 이러한 분산된 데이터셋을 서버(server)에서 수집하여 모델을 훈련시킨다는 점에서 중앙 집중적인 특성을 가진다. 그러나 데이터셋을 수집하는 과정에서 서버에 대규모의 통신 부하가 발생할 뿐만 아니라, 디바이스들의 개인정보가 그대로 전송된다는 점에서 심각한 개인정보 유출의 위협이 발생한다는 한계점을 가진다[3].

이러한 중앙 집중적 방식의 한계점을 극복하기 위해, 연합학습(federated learning)이 제안되었다[4]. 연합학습에서는 개별 디바이스 또는 클라이언트(client)가 개별 데이터셋을 이용하여 로컬 모델(local model)을 학습시킨다. 그리고 학습된 로컬 모델 파라미터(local model parameter) 또는 그래디언트(gradient)를 서버에 전송하고, 서버는 전송받은 정보를 집계(aggregation)하여 전역 모델 파라미터(global model parameter)를 업데이트한다. 클라이언트의 데이터셋을 직접 공유하지는 않으면서도 데이터셋의 특성을 학습한 모델 파라미터를 공유함으로써 대규모 데이터셋을 간접적·분산적으로 활용하는 효율적인 머신러닝 방식이 제안된 것이다.

하지만 연합학습은 서버에 비해 제한적인 연산 및 통신 자원을 가진 클라이언트에게 로컬 모델을 학습시키고 전송하도록 요구한다는 점에서, 클라이언트에게 연산 및 통신 자원에 대한 오버헤드(overhead)를 발생시킨다[3,7-9]. 따라서 실제 연합학습 시스템에서는 클라이언트가 연합학습에 참여하지 않기로 선택하는 경우가 발생할 수 있다. 또한 실제 연합학습 시스템에서 클라이언트는 이질성(heterogeneity)를 가지고 있으므로, 클라이언트 데이터셋의 질(quality)과 양(quantity)에 따라 집계된 전역 모델의 성능이 저하될 수 있다는 한계점이 있다[5-11].

이러한 한계점을 극복하기 위해, 연합학습의 성능 개선에 기여할 클라이언트를 선택하는 클라이언트 선택 전략(client selection strategy), 연합학습 참가에 대한 비용을 보상하는 보상 분배 메커니즘(payment allocation mechaism), 그리고 이 두 가지를 모두 포함하는 인센티브 메커니즘(incentive mechanism)들이 제안되었다[8,9,12,13]. 클라이언트 선택 전략 연구에서는 클라이언트의 로컬 모델 손실(loss)[8], 소모비용[9] 등을 고려하여 연합학습의 정확도 및 수렴 속도를 개선하는 방식이 제안되어 왔으며, 보상 분배 메커니즘에서는 클라이언트의 소모비용, 기여도[12] 등을 고려하여 보상을 측정하는 방식이 제안되어 왔다. 또한, 인센티브 메커니즘에서는 클라이언트의 정보를 보호하기 위해, 차분 프라이버시(differential privacy)를 적용하는 프라이버시 보호 인센티브 메커니즘들도 제안되었다[14-16]. 차분 프라이버시란 클라이언트의 정보 보호 요구 수준에 따라 로컬 모델 파라미터에 노이즈를 추가하여 전송하도록 허용하는 방식이다. 그러나 기존에 제안된 클라이언트 선택 전략, 보상 분배 메커니즘 및 인센티브 메커니즘은 클라이언트의 로컬 모델의 성능이나 자원, 차분 프라이버시의 정도 등의 다차원적인 기기정보[13]를 서버에게 전송하도록 요구한다는 점에서, 클라이언트의 정보를 노출하지 않는다는 연합학습의 근본적인 원칙에 부합하지 않는다는 한계점이 존재한다.

따라서 본 논문에서는 클라이언트의 기기정보를 공유하지 않아도 되는 인센티브 메커니즘을 제안하고자 한다. 제안하는 인센티브 메커니즘에서 클라이언트는 연합학습 수행에 소모하는 비용과 로컬 모델의 자체 평가된 성능을 반영하여 받고자 하는 최소 보상정보만을 서버에게 전송함으로써, 기기정보가 구분되지 않는 정보만을 서버에게 전송하게 된다. 이후 서버는 전송받은 최소 보상정보를 비교하여 클라이언트 선택을 수행하며, 분배할 보상을 결정하기 위해 순차적으로 제안을 주고 받는 교대 제안 협상[17]을 수행한다. 이를 통해 클라이언트의 기기정보가 구분되지 않는 방식으로 연합학습의 성능을 개선할 수 있는 클라이언트를 선택하고, 소모비용을 보상하여 안정적인 연합학습 시스템을 구성 할 수 있다. 실험을 통해 제안하는 인센티브 메커니즘은 클라이언트의 기기정보 없이도 연합학습의 수렴 속도 및 테스트 정확도(test accuracy)를 개선하며, 최적의 자원 분배 지점을 근사할 수 있음을 보였다.

본 논문은 다음과 같이 구성된다. Ⅱ장에서는 연합학습 시스템 및 서버와 클라이언트의 효용 함수를 모델링하고, 인센티브 메커니즘의 문제를 정의한다. Ⅲ장에서는 기기정보를 활용하지 않는 클라이언트 선택 전략과 보상 분배 방식을 포함하는 인센티브 메커니즘을 제안한다. Ⅳ장에서는 실험을 통해 제안하는 인센티브 메커니즘의 성능을 검증하며, Ⅴ장에서는 본 논문을 결론 맺는다.

Ⅱ. 시스템 모델링 및 문제 정의

2.1 연합학습 시스템 모델링

본 논문에서는 하나의 서버와 다수의 클라이언트가 존재하는 연합학습 시스템을 고려한다. 서버와 클라이언트들은 동일한 구조를 가진 인공지능 모델을 가지고 있으며 서버는 시스템의 평균적인 모델 성능을 향상시키고자 한다.

연합학습 시스템의 라운드 $t(t=0,1,\cdots,T)$에서 클라이언트 $i\in\boldsymbol{n}(t)=\{1,2,\cdots,n(t)\}$의 로컬 모델 파라미터를 $\boldsymbol{w}_i(t)$, 개별 데이터셋의 크기를 $|D_i|$, 개별 손실함수를 $F_i(\boldsymbol{w}_i(t))$라고 하자. 서버 S는 시스템 내 평균적인 모델 성능을 향상시키는 전역 모델 파라미터 $\boldsymbol{w}(t)$를 찾기 위해, 클라이언트의 개별 목적함수 $F_i(\boldsymbol{w}(t))$를 조합한 전역 손실함수 $F(\boldsymbol{w}(t))$를 최소화하는 것을 목적으로 한다.

$$F(\boldsymbol{w}(t))=\sum_{i=1}^{n(t)}p_iF_i(\boldsymbol{w}(t)), \tag{1}$$

이때 $p_i=|D_i|/\sum_{i=1}^{n(t)}|D_i|$로, 클라이언트의 상대적인 데이터셋의 크기를 반영한다. 식 (1)의 전역 손실함수를 최소화하기 위해, 서버 S는 클라이언트 중 일부를 선택하여 로컬 모델을 학습시키고 서버에 모델 파라미터를 전송하는 태스크(task)를 부여한다. 이때 서버 S는 주요한 클라이언트의 반복적인 연합학습 참가를 유도하기 위해, 선택된 클라이언트에게 태스크 수행에 소모하는 비용에 대한 보상자원 $x_i(t)$를 분배한다. 서버 S는 전송 받은 모델 파라미터를 조합하는 방식으로 전역 모델 파라미터를 업데이트하여 시스템 내에서 범용적으로 작동하는 전역 모델을 얻을 수 있다. 본 논문에서는 전역 모델의 업데이트 방식으로 FedAvg (federated averaging)[4]를 사용한다. 인센티브 메커니즘을 통해 선택된 클라이언트의 집합을 $\boldsymbol{C}(t)$라 하면, 전역 모델 파라미터 $\boldsymbol{w}(t)$는 다음과 같이 업데이트된다.

$$\boldsymbol{w}(t)=\sum_{i\in\boldsymbol{C}(t)}p_i\boldsymbol{w}_i(t). \tag{2}$$

업데이트된 전역 모델 파라미터 $\boldsymbol{w}(t)$는 시스템 내 클라이언트에게 전송됨으로써 연합학습의 라운드 t가 종료된다. 그림 1은 인센티브 메커니즘을 포함한 연합학습 시스템을 나타낸다.

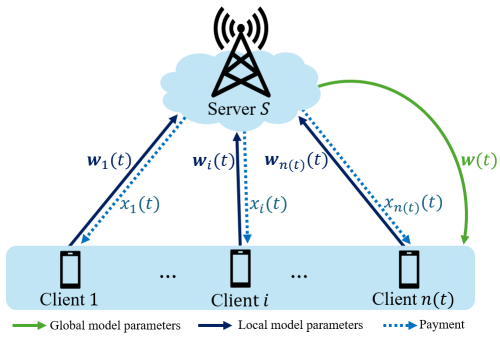


그림 1. 인센티브 메커니즘을 포함한 연합학습 시스템
Fig. 1. Federated learning system with an incentive mechanism

2.1.1 서버의 효용 모델링

연합학습 시스템의 라운드 t에서 $n(t)$명의 클라이언트가 존재할 때 연합학습에 참가시키고자 하는 클라이언트의 비율을 $K(0\le K\le 1)$라고 하면, 서버 S는 $\lfloor Kn(t)\rfloor$명의 클라이언트를 선택하여 연합학습을 수행시키고 그에 대한 대가로 보상자원을 분배하며, 클라이언트의 선택 비율 K는 서버의 통신 능력에 따라 결정된다[18]. 서버 S가 활용 가능한 총 보상자원 $R(t)$는 라운드 t에서의 보상자원 예산 $R_S(t)$와 직전 라운드 $t-1$에서 남은 보상자원 $r(t-1)$의 합으로 결정된다 $(R(t)=R_S(t)+r(t-1))$.

서버 S는 연합학습을 통해 얻을 것으로 기대되는 전역 모델의 정확도 이득(accuracy gain) $G(t)$[9]와 연합학습 과정에서 모델 파라미터 송수신에 소모할 것으로 예상되는 통신 자원 오버헤드로 구성된 소모비용 $\phi_S(t)$[7]를 고려하여, 참가할 클라이언트를 선택하고 활용 가능한 보상자원 $R(t)$를 분배한다. 이때 서버의 소모비용 $\phi_S(t)$는 모델 파라미터 송수신에 소모되는 통신 자원 오버헤드 및 모델 파라미터 집계에 소모되는 연산 자원 오버헤드로 구성되며, 참가 클라이언트의 수가 클수록 통신 자원 오버헤드가 지배적이다[6]. 정확도 이득 $G(t)$는 초기 전역 모델의 정확도 대비 라운드 t에서의 정확도의 차이를 의미한다. 라운드 t에서 전역 모델의 정확도를 $g(\boldsymbol{w}(t))$, 정확도 차이에 대한 주관적 만족도를 $\lambda(\lambda>0)$라 할 때, 정확도 이득 $G(t)$는 다음과 같이 정의된다.

$$G(t)=\lambda(g(\boldsymbol{w}(t))-g(\boldsymbol{w}(0))). \tag{3}$$

이때 인센티브 메커니즘에서는 연합학습 수행 이전에 클라이언트를 선택하고 분배할 보상을 결정하므로,

정확도 이득 $G(t)$를 예측하기 위해 직전 두 라운드에서 정확도 이득의 평균값을 이용한다($G(t)=(G(t-1)+G(t-2))/2$).

인센티브 메커니즘을 통해 서버 S가 선택한 클라이언트의 집합 $\boldsymbol{C}(t)$에 분배할 보상자원의 벡터를 $\boldsymbol{x}(t)=(x_i(t),\cdots,x_j(t)),(i,\cdots,j\in\boldsymbol{C}(t))$라 하자. 이때 서버 S의 효용 $u_S(\boldsymbol{x}(t))$은 다음과 같이 정의된다.

$$u_S(\boldsymbol{x}(t))=G(t)-\phi_S(t)-\sum_{i\in\boldsymbol{C}(t)}x_i(t). \tag{4}$$

2.1.2 클라이언트의 효용 모델링

연합학습 시스템 내의 클라이언트 i는 로컬 모델을 활용하는 임의의 서비스를 이용하므로, 로컬 모델의 성능에 대한 자체적인 평가를 수행한다. 이때 클라이언트 i는 연합학습 참가 시 기대되는 자신의 기여도를 자체적으로 측정하며, 이를 자체 평가 성능(self estimated performance) $e_i(t)$라고 정의한다. 자체 평가 성능 $e_i(t)$는 로컬 모델의 손실 $F_i(\boldsymbol{w}_i(t))$와 로컬 모델 훈련에 소요되는 시간에 영향을 미쳐 클라이언트의 연산 자원 오버헤드를 증가시키는 데이터셋의 크기 $|D_i|$[8]를 복합적으로 고려하도록 다음과 같이 정의한다.

$$e_i(t)=\frac{\gamma_i}{F_i(\boldsymbol{w}_i(t))}\times\frac{\mu_i}{|D_i|}, \tag{5}$$

이때 $\gamma_i(\gamma_i>0)$는 로컬 모델의 손실에 대한 주관적 민감도, $\mu_i(\mu_i>0)$는 훈련 시간에 대한 주관적 민감도를 나타낸다.

클라이언트 i가 연합학습에 참가한다면, 파라미터 송수신에 필요한 통신 자원 오버헤드뿐만 아니라 로컬 모델 훈련에 필요한 연산 자원 오버헤드를 포함하는 비용 $\phi_i(t)$를 소모한다[3,7]. 따라서 클라이언트 i는 비용 $\phi_i(t)$를 보상 받으면서 로컬 모델의 자체 평가 성능 $e_i(t)$에 대응되는 보상자원 $x_i(t)$를 얻고자 한다. 따라서 클라이언트 i의 효용 $u_i(x_i(t))$는 다음과 같이 정의된다.

$$u_i(x_i(t))=x_i(t)+e_i(t)-\phi_i(t). \tag{6}$$

2.2 클라이언트 선택 및 보상자원 분배 문제 정의

인센티브 메커니즘의 클라이언트 선택 문제는 사회 후생 최대화(social welfare maximization) 문제로 정의할 수 있으며, 사회 후생은 서버와 클라이언트의 효용의 합으로 정의된다[9].

$$\arg\max_{\boldsymbol{C}(t)} u_S(\boldsymbol{x}(t))+\sum_{i\in\boldsymbol{C}(t)}u_i(x_i(t)). \tag{7}$$

또한, 인센티브 메커니즘의 보상자원 분배 문제는 내쉬 협상 해법(Nash bargaining solution)을 찾는 문제로 정의할 수 있다[19]. 내쉬 협상 해법은 연합학습에 참가한 클라이언트의 효용의 곱으로 정의되는 시스템 효용 또는 내쉬 곱(NP, Nash product)을 최대화하는 지점과 일치한다[20]. 따라서 내쉬 협상 해법은 다음과 같이 정의할 수 있다.

$$\arg\max_{\boldsymbol{x}(t)}\prod_{i\in\boldsymbol{C}(t)}(u_i(x_i(t))-d_i), \tag{8}$$

이때 d_i는 클라이언트 i가 얻고자 하는 최소 효용인 불일치점(disagreement point)을 나타낸다[21].

Ⅲ. 인센티브 메커니즘

본 논문에서는 클라이언트의 기기정보 공유 없이 연합학습에 기여할 클라이언트를 선택하고 할당할 보상을 결정하는 인센티브 메커니즘을 제안한다. 제안하는 인센티브 메커니즘은 서버의 최대 보상정보 공지 및 클라이언트의 최소 보상정보 전송, 서버의 클라이언트 선택, 서버와 클라이언트의 교대 제안 협상, 그리고 서버의 클라이언트 추가 선택의 순으로 동작한다.

3.1 서버의 최대 보상정보 공지 및 클라이언트의 최소 보상정보 전송

서버 S는 모든 클라이언트에게 연합학습에 참가한다면 할당받을 수 있는 최대 보상정보 $R_{S,i}(t)$를 공지한다. 이때 공정한 보상자원 분배를 유도하기 위해, 최대 보상정보 $R_{S,i}(t)$는 총 보상자원 $R(t)$를 선택하고자 하는 $\lfloor Kn(t)\rfloor$명 클라이언트에게 균일하게 분배하는 값으로 설정한다.

$$R_{S,i}(t)=\frac{R(t)}{\lfloor Kn(t)\rfloor}. \tag{9}$$

클라이언트 i는 연합학습에 참가한다면 받고자 하는 최소 보상정보 $R_{i,S}(t)$를 계산하여 서버 S에 전송한다. 이때 최소 보상정보 $R_{i,S}(t)$는 클라이언트 i의 효용 $u_i(x_i(t))$가 0이 되는 지점에서의 보상자원 $x_i(t)$의 값

으로 설정한다.

$$R_{i,S}(t)=\phi_i(t)-e_i(t), \tag{10}$$

이는 클라이언트 i의 불일치점 d_i에 도달할 수 있는 보상자원 $x_i(t)$에 대응된다. 제안하는 인센티브 메커니즘에서는 자체 평가 성능 $e_i(t)$와 소모비용 $\phi_i(t)$를 반영한 최소 보상정보 $R_{i,S}(t)$만을 서버 S에게 전송함으로써, 실제 클라이언트의 기기정보인 로컬 모델 손실 $F_i(\boldsymbol{w}_i(t))$, 데이터셋의 크기 $|D_i|$와 소모비용 $\phi_i(t)$의 값을 드러내지 않을 수 있다.

3.2 서버의 클라이언트 선택

서버 S는 클라이언트 i로부터 전송받은 최소 보상정보 $R_{i,S}(t)$와 자신이 공지했던 최대 보상정보 $R_{S,i}(t)$를 비교하여, 다음과 같이 후보자 클라이언트 집합 $\boldsymbol{C}'(t)$를 결정한다.

$$\boldsymbol{C}'(t)=\{\, i\in\boldsymbol{n}(t) \mid R_{i,S}(t)\le R_{S,i}(t)\,\}. \tag{11}$$

이때 후보자 클라이언트 집합의 크기를 $|\boldsymbol{C}'(t)|$라 하고, 집합 내 클라이언트의 최소 보상정보 $R_{i,S}(t)$를 오름차순으로 나열하면 $R^1_{i,S}\le\cdots\le R^m_{j,S}\le\cdots\le R^{|\boldsymbol{C}'(t)|}_{l,S}$라 하자. 만약 $|\boldsymbol{C}'(t)|>\lfloor Kn(t)\rfloor$이면, 서버 S는 아래의 조건을 만족하도록 선택하는 클라이언트의 집합 $\boldsymbol{C}(t)$를 결정한다.

$$\boldsymbol{C}(t)=\{\, i\in\boldsymbol{C}'(t) \mid m\le\lfloor Kn(t)\rfloor\,\}. \tag{12}$$

만약 $|\boldsymbol{C}'(t)|<\lfloor Kn(t)\rfloor$이면, 선택하는 클라이언트의 집합을 후보자 클라이언트의 집합으로 결정한다 ($\boldsymbol{C}(t)=\boldsymbol{C}'(t)$). 서버 S는 선택된 클라이언트의 집합 $\boldsymbol{C}(t)$에 대한 보상자원 분배 이후에, 선택되지 않은 클라이언트 중 $\lfloor Kn(t)\rfloor-|\boldsymbol{C}(t)|$명을 추가로 선택할 수 있다. 이는 Ⅲ장 4절에서 이어진다.

3.3 서버와 클라이언트의 교대 제안 협상

서버 S와 클라이언트는 보상자원 분배 지점 $\boldsymbol{x}(t)$를 결정하기 위해, 교대 제안 협상을 수행한다.

3.3.1 협상 분해 및 교대 제안 협상

본 논문에서는 교대 제안 협상의 복잡도를 낮추기 위해, 서버 S와 $|\boldsymbol{C}(t)|$명 클라이언트의 교대 제안 협상을 서버 S와 각 클라이언트 $i(i\in\boldsymbol{C}(t))$의 독립적인 $|\boldsymbol{C}(t)|$개의 교대 제안 협상으로 분해한다. 이를 위해 서버 S가 각 클라이언트 i의 참가를 통해 얻는 효용 $u_{S,i}(x_i(t))$를 다음과 같이 정의한다.

$$u_{S,i}(x_i(t))=\frac{G(t)+\phi_S(t)}{|\boldsymbol{C}(t)|}-x_i(t). \tag{13}$$

분해된 교대 제안 협상에서 서버 S와 각 클라이언트 i는 보상 $x_i(t)$를 결정하고자 한다. 서버 S와 클라이언트 i는 제안시점 $\alpha_i(\alpha_i=0,1,...,A_i)$이 진행됨에 따라 순차적으로 어느 한쪽은 제안 $x_i(\alpha_i)$을 하고, 나머지 한쪽은 제안에 대한 의사결정을 수행한다. 만약 제안 $x_i(\alpha_i)$가 거절되면 다음 제안시점 α_i+1이 진행되며, 서버 S와 클라이언트 i의 효용은 각각 할인계수 (discount factor) $\delta_S,\delta_i(\delta_S,\delta_i\in[0,1))$배로 감소한다. 할인계수는 협상이 지연되기보다는 빠르게 성사되는 것을 선호하는 특성을 나타낸다[22]. 할인계수의 값이 0에 가까울수록 협상 지연에 대한 인내심(patience)이 없음을 의미하며, 할인계수의 값이 1에 가까울수록 협상 지연에 대해 완벽한 인내심이 있다는 것을 의미한다.

만약 제안 $x_i(\alpha_i)$가 수락되면 협상이 종료되고 $(A_i=\alpha_i)$, 보상 $x_i(t)$가 결정된다$(x_i(t)=x_i(A_i))$. 이때 결정된 보상 $x_i(t)$가 서버 S의 최대 보상정보 $R_{S,i}(t)$에 비해 작다면, 클라이언트 i와의 협상에서 남는 보상 $r_i(t)$는 다음과 같이 결정된다.

$$r_i(t)=R_{S,i}(t)-x_i(t). \tag{14}$$

분해된 $|\boldsymbol{C}(t)|$개의 독립적인 교대 제안 협상은 동시적으로 진행되므로, 클라이언트의 협상 종료 시점 A_i는 서로 다를 수 있다. 따라서 분해된 교대 제안 협상을 적용한 보상자원 분배 문제는 다음과 같이 재정의된다.

$$\arg\max_{\boldsymbol{x}(t)}\prod_{i\in\boldsymbol{C}(t)}\left(\delta_i^{A_i}u_i(x_i(t))-d_i\right). \tag{15}$$

3.3.2 적응적 교대 제안 협상 전략

서버 S는 효율적 협상 타결을 유도하기 위해, 자신의 할인계수 δ_S를 클라이언트 i에게 알린 후에 교대 제안 협상을 수행한다. 교대 제안 협상의 제안시점 α_i에서 클라이언트 i가 보상 $x_i(\alpha_i)$를 제안할 차례라 가정하자.

클라이언트 i는 서버 S의 수락을 유도하기 위해, 자

신의 직전 제안 $x_i(\alpha_i-2)$에 비해 자신의 효용을 감소시켜 서버 S에게 양보하는 제안을 한다. 이때 효용 감소 간격 $\triangle_i$은 서버 S의 할인계수에 대해 적응적으로 조정하기 위해, 할인계수의 비(δ_S/δ_i)에 비례하게 설정한다. 이러한 반대제안 전략은 다음과 같이 정의된다.

$$\delta_i^{\alpha_i}u_i(x_i(\alpha_i))=\delta_i^{\alpha_i}u_i(x_i(\alpha_i-2))-\triangle_i, \quad \left(\triangle_i=\beta_i\frac{\delta_S}{\delta_i}\right). \tag{16}$$

이때 β_i는 협상에서 클라이언트 i의 양보율을 의미한다.

서버 S는 클라이언트 i에게 제안 $x_i(\alpha_i)$을 받으면, 자신의 효용을 고려하여 의사결정을 수행한다. 현재 받은 제안의 효용이 자신의 직후 제안 시점인 α_i+1에서 제안가능한 최대 효용보다 크거나 같으면, 제안을 수락한다. 이러한 의사결정 기준은 다음과 같이 표현할 수 있다.

$$\begin{cases}\text{Accept,} \\ \text{if } \delta_S^{\alpha_i}u_{Si}(x_i(\alpha_i))\geq\delta_S^{\alpha_i+1}u_{Si}(x_i(\alpha_i-1))-\triangle_S, \\ \text{Reject,} \\ \text{otherwise.}\end{cases} \tag{17}$$

이때 서버 S는 클라이언트 i의 기기정보인 할인계수 δ_i를 알지 못하므로, 효용 감소 간격 $\triangle_S$은 자신의 할인계수만을 기반으로 결정한다. 따라서 서버 S의 양보율을 β_S라 하면, 효용 감소 간격 $\triangle_S$는 다음과 같다.

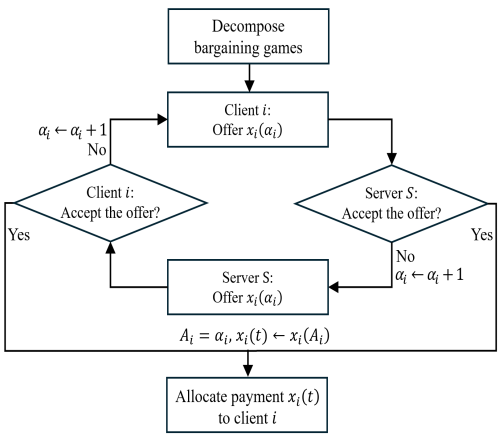


그림 2. 제안하는 교대 제안 협상의 동작 과정
Fig. 2. Process of the proposed alternating-offers bargaining

$$\triangle_S=\frac{\beta_S}{\delta_S}. \tag{18}$$

만약 제안 $x_i(\alpha_i)$이 수락되지 않아 다음 제안시점이 진행되면, 서버 S는 동일한 방식으로 반대제안을 수행하고, 클라이언트 i는 의사결정을 수행한다. 그림 2는 제안하는 교대 제안 협상의 동작 과정을 간략히 나타낸다.

3.4 서버의 클라이언트 추가 선택

Ⅲ장 2절에서 언급되었듯, 만약 $\min(\lfloor Kn(t)\rfloor, |\boldsymbol{C}(t)|)=|\boldsymbol{C}(t)|$이면, 서버 S는 거절했던 클라이언트$(i\notin\boldsymbol{C}(t))$에 대한 추가 선택을 시도한다. 서버 S는 이미 선택했던 클라이언트에 대한 보상 분배 후에 남은 보상자원을 활용하기 위해, 최대 보상정보 $R_{S,i}(t)$를 다음과 같이 업데이트한다.

$$R_{S,i}(t)=\frac{R(t)}{\lfloor Kn(t)\rfloor}+\frac{\sum_{i\in\boldsymbol{C}(t)}r_i(t)}{\lfloor Kn(t)\rfloor-|\boldsymbol{C}(t)|}. \tag{19}$$

업데이트된 최대 보상정보 $R_{S,i}(t)$를 이용하여, 서버 S는 Ⅲ장 2절의 클라이언트 선택 및 Ⅲ장 3절의 교대 제안 협상을 추가로 수행한다. 이러한 과정은 남은 보상자원을 활용하더라도 더 이상 클라이언트가 추가로 선택되지 않을 때까지 최대 $\lfloor Kn(t)\rfloor$번 반복되며, 보상정보만이 전송되므로 모델 파라미터 송·수신에 비해 무시할만한 오버헤드를 가진다[18]. 추가 선택이 종료된 이후 남은 보상자원 $r(t)=\sum_{i\in\boldsymbol{C}(t)}r_i(t)$는 다음 라운드 $t+1$에서 활용된다.

Ⅳ. 실험 및 성능 검증

4.1 실험 설정

Ⅲ장에서 제안한 인센티브 메커니즘의 클라이언트 선택 전략과 보상 분배 방식의 성능을 검증하기 위해 실험에서 활용된 조건 및 파라미터 설정 값들을 표 1에서 나타내었다.

클라이언트 선택 전략의 비교 알고리즘으로는 손실이 큰 순서로 클라이언트를 선택하는 pow-d (power of choice)[8]을 사용하였으며, 클라이언트 선택을 위한 후보자 클라이언트 집합의 크기 d를 16으로 설정하였다. 공정한 성능 비교를 위해 60라운드의 연합학습을 15번

표 1. 실험에서 활용된 조건 및 파라미터 설정
Table 1. Conditions and parameter settings in the experiment

Category	Element	Details
Dataset and Model	Dataset	Fashion-MNIST[23]
	Data Heterogeneity	$Dir(0.1)$, Dirichlet distribution
	Model	LeNet-5[24]
	Learning Rate	0.01
Server	λ	1200
	$\phi_S(t)$	1
	$R(t)$	$[550,1100]$, Uniform distribution
Client	γ_i	$N(105,1)$, Gaussian distribution
	μ_i	$N(5500,1)$, Gaussian distribution
	ϕ_i	$[0,2]$, Uniform distribution
Hyper Parameter	δ_S,δ_i	$\{0.6,0.7,0.8,0.9\}$, Uniform distribution
	β_S,β_i	$[0.00008,0.002]$, Uniform distribution

반복하여 평균적 성능을 비교하였다.

보상 분배 방식의 내쉬 협상 해법에 대한 근사 성능을 검증하기 위해, 클라이언트의 효용 함수를 이용하여 내쉬 협상 해법을 계산하는 DV (direction vector) 기반 알고리즘[25]을 사용하였으며 500번을 반복하여 평균적 성능을 측정하였다.

4.2 실험 결과

제안하는 클라이언트 선택 전략에 따른 연합학습의 정확도와 수렴 속도를 검증하고자 한다. 그림 3은 라운드 t가 진행될 때 클라이언트 선택 전략에 따른 평균적인 클라이언트 모델의 정확도를 나타내며, 표 2는 클라이언트 선택 전략에 따른 목표 정확도(target accuracy) 75% 도달에 소요되는 라운드 수(t_{75})와 테스트 정확도를 나타낸다. 평균적인 클라이언트의 정확도에 관하여, pow-d 전략의 최종 테스트 정확도는 79.25%에 도달하는 반면, 제안하는 클라이언트 선택 전략의 최종 테스트 정확도는 평균 80.19%로 더 높은 수준에 도달하는 것을 확인할 수 있다. 또한 수렴 속도의 경우, pow-d 전략은 16라운드가 소요되지만, 제안하는 클라이언트 선택 전략은 8라운드가 소요되어 수렴 속도가 2배로 증가한다. 이를 통해 제안하는 클라이언트 선택 전략은 자체

표 2. 클라이언트 선택 전략에 따른 t_{75}와 최종 테스트 정확도 [%]
Table 2. t_{75} and test accuracy [%] according to the client selection strategies

	Pow-d, d=16[8]	Proposed mechanism
t_{75}	16	8
Test acc.	79.25	80.19

평가 성능을 활용함으로써 로컬 모델 손실이나 데이터셋 크기 등의 기기정보를 드러내지 않고도 효율적인 연합학습을 가능하게 함을 확인할 수 있다. 다만 제안하는 클라이언트 선택 전략의 표준 편차(STD, standard deviation)는 비교적 크게 나타나는데, 이는 클라이언트 선택 과정에서 가우시안 분포(Gaussian distribution)으로부터 확률적으로 추출되는 민감도 γ_i, μ_i를 활용하면서 변동성이 발생하는 것으로 추측할 수 있다.

또한, 제안하는 교대 제안 협상 전략을 활용한 보상 분배 방식의 내쉬 협상 해법에 대한 근사 성능을 평가하고자 한다. 표 3은 연합학습에 선택된 클라이언트 수 $|\boldsymbol{C}(t)|$가 집합 $\{2,5,8,11\}$에서 결정될 때, 제안하는 교대 제안 협상 전략에 따른 자원 분배 지점에서의 내쉬 곱과 DV 기반 알고리즘의 내쉬 곱, 그리고 두 지점 사이의 절대 백분율 오차(APE, absolute percentage error)와 APE의 STD를 나타낸다. 연합학습에 참가하는 클라이언트의 수가 순차적으로 증가함에 따라, 제안하는 교대 제안 협상 전략의 내쉬 협상 해법에 대한 APE는 0.0003%, 0.0040%, 0.0148%, 0.0369%으로 증가하고, STD는 0.0009, 0.0058, 00014, 0.0030으로 증가하지만, 각각 0.05%와 0.005 이내의 낮은 값을 유지한다.

이러한 경향성은 선택된 클라이언트의 수가 증가함에 따라 협상의 분해에서 오차가 발생하며, 클라이언트의 양보율 β_i가 균일 분포(uniform distribution)에서 확

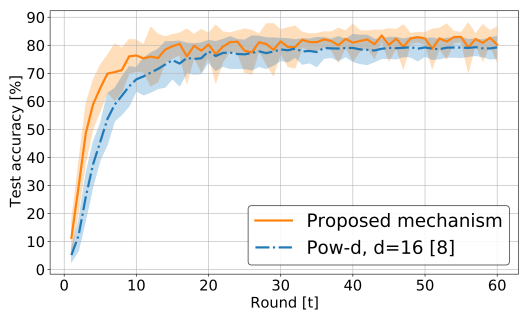


그림 3. 클라이언트 선택 전략에 따른 평균 테스트 정확도
Fig. 3. Average test accuracy according to the client selection strategies

표 3. $|\mathcal{C}(t)|$가 증가할 때 보상 분배 방식에 따른 NP와 내쉬 협상 해법에 대한 APE [%]와 STD
Table 3. NP, APE [%] between the two NPs, and STD of the APE according to the payment allocation strategies when $|\mathcal{C}(t)|$ increases

Method		NP		APE [%]	STD
		DV-based[25]	Proposed		
$\|\mathcal{C}(t)\|$	2	5.96×10^{4}	5.96×10^{4}	0.0003	0.0009
	5	1.11×10^{10}	1.11×10^{10}	0.0040	0.0058
	8	3.79×10^{14}	3.79×10^{14}	0.0148	0.0014
	11	4.84×10^{18}	4.84×10^{18}	0.0369	0.0030

률적으로 추출될 때 변동성이 발생하는 것으로 추측할 수 있다. 이를 통해 제안하는 교대 제안 협상 전략이 클라이언트의 수가 증가할 때 오차 및 변동성이 발생하는 특성이 있지만, 클라이언트의 기기정보 공유 없이 낮은 오차율로 내쉬 협상 해법을 근사할 수 있다는 것을 확인할 수 있다.

V. 결 론

본 논문에서는 연합학습에서 클라이언트의 자체 평가 성능을 반영하는 최소 보상정보를 기반으로 한 클라이언트 선택 전략과 협상 분해 및 교대 제안 협상을 기반으로 한 보상 분배 방식을 포함하는 인센티브 메커니즘에 대한 연구를 진행하였다. 클라이언트의 로컬 모델 손실 및 데이터셋 크기를 고려하여 자체 평가 성능을 정의하였으며, 이를 반영한 최소 보상정보를 공유함으로써 클라이언트의 실제 기기정보가 드러나지 않고도 클라이언트 선택이 이루어지는 전략을 제안하였다. 또한 선택된 클라이언트에 대한 보상자원 분배를 위해 협상을 분해하여 서버와 클라이언트의 교대 제안 협상을 적용하였으며, 서버의 할인계수를 활용한 적응적인 교대 제안 협상 전략을 제안하였다. 클라이언트 선택 전략에 대한 실험을 통해 제안된 클라이언트 선택 전략은 서버가 클라이언트의 손실을 활용하는 기존의 전략에 비해 연합학습의 정확도가 개선되고 수렴 속도가 증가하는 것을 확인하였다. 또한 보상 분배 방식에 대한 실험을 통해 제안된 교대 제안 협상 전략이 낮은 오차율로 내쉬 협상 해법에 대해 근사한다는 것을 확인하였다. 따라서 제안하는 인센티브 메커니즘을 통해 클라이언트의 기기정보를 공유하지 않고도 연합학습의 성능을 개선하고 효율적인 보상자원 분배를 수행할 수 있음을 확인하였다.

References

[1] T. H. Rafi, S. Y. Lim, and D. Chae, "A survey on federated learning and its business applications," *Commun. Korean Inst. Inf. Sci. and Eng.*, vol. 42, no. 9, pp. 21-27, Sep. 2024.

[2] T. B. Ahammed, R. Patgiri, and S. Nayak, "A vision on the artificial intelligence for 6G communication," *ICT Exp.*, vol. 9, no. 2, pp. 197-210, Apr. 2023. (https://doi.org/10.1016/j.icte.2022.05.005.)

[3] A. Imteaj, U. Thakker, S. Wang, J. Li, and M. H. Amini, "A survey on federated learning for resource-constrained IoT devices," *IEEE Internet of Things J.*, vol. 9, no. 1, pp. 1-24, Jan. 2022. (https://doi.org/10.1109/JIOT.2021.3095077)

[4] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proc. 20th Int. Conf. Artif. Intell. Statist. (AISTATS 2017)*, pp. 1273-1282, Ft. Lauderdale, FL, USA, Apr. 2017.

[5] J. Lee and H. Ko, "Adaptive federated learning in non-IID data environment," *J. KICS*, vol. 49, no. 8, pp. 1118-1120, Aug. 2024. (https://doi.org/10.7840/kics.2024.49.8.1118)

[6] M. K. Nori, S. Yun, and I.-M. Kim, "Fast federated learning by balancing communication trade-offs," *IEEE Trans. Commun.*, vol. 69, no. 8, pp. 5168-5182, Aug. 2021. (https://doi.org/10.1109/TCOMM.2021.3083316)

[7] J. Wen, Z. Zhang, Y. Lan, Z. Cui, J. Cai, and W. Zhang, "A survey on federated learning: Challenges and applications," *Int. J. Mach. Learn. Cybern.*, vol. 14, no. 2, pp. 513-535, Feb. 2023. (https://doi.org/10.1007/s13042-022-01647-y)

[8] Y. J. Cho, J. Wang, and G. Joshi, "Towards understanding biased client selection in federated learning," in *Proc. 25th Int. Conf. Artif. Intell. Statist. (AISTATS 2022)*, pp. 10351-10375, Valencia, Spain, Mar. 2022.

[9] Y. Li, F. Li, S. Yang, C. Zhang, L. Zhu, and Y. Wang, "A cooperative analysis to incentivize communication-efficient federated learning," *IEEE Trans. Mobile Comput.*, vol. 23, no. 10, pp. 10175-10190, Oct. 2024. (https://doi.org/10.1109/TMC.2024.3373501)

[10] H. Park, M. Kim, and M. Kwon, "Personalized federated sensing for heterogeneous environment," *IEEE Sensors Lett.*, vol. 9, no. 4, pp. 1-4, Apr. 2025. (https://doi.org/10.1109/LSENS.2024.3464518)

[11] Z. Cheng, et al. "Learning-based client selection for multiple federated learning services with constrained monetary budgets," *ICT Express*, vol. 9, no. 6, pp. 1059-1064, Feb. 2023. (https://doi.org/10.1016/j.icte.2023.01.007)

[12] H. Yu, et al., "A sustainable incentive scheme for federated learning," *IEEE Intell. Syst.,* vol. 35, no. 4, pp. 58-69, Jul.-Aug. 2020. (https://doi.org/10.1109/MIS.2020.2987774)

[13] N. Ding, Z. Fang, and J. Huang, "Optimal contract design for efficient federated learning with multi-dimensional private information," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 1, pp. 186-200, Jan. 2021. (https://doi.org/10.1109/JSAC.2020.3036944)

[14] D. Wang, J. Ren, Z. Wang, Y. Wang, and Y. Zhang, "PrivAim: A dual-privacy preserving and quality-aware incentive mechanism for federated learning," *IEEE Trans. Comput.*, vol. 72, no. 7, pp. 1913-1927, Jul. 2023. (https://doi.org/10.1109/TC.2022.3230904)

[15] P. Sun, H. Che, Z. Wang, Y. Wang, T. Wang, and L. Wu, "Pain-FL: Personalized privacy preserving incentive for federated learning," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 12, pp. 3805-3820, Dec. 2021. (https://doi.org/10.1109/JSAC.2021.3118354)

[16] T. Liu, B. Di, P. An, and L. Song, "Privacy-preserving incentive mechanism design for federated cloud-edge learning," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 3, pp. 2588-2600, Jul.-Sep. 2021. (https://doi.org/10.1109/TNSE.2021.3100096)

[17] B. An, N. Gatti, and V. Lesser, "Alternating-offers bargaining in one-to-many and many-to-many settings," *Annals Math. Artif. Intell.*, vol. 77, no. 1, pp. 67-103, Jun. 2016. (https://doi.org/10.1007/s10472-016-9506-x)

[18] G. S. Nariman and H. K. Hamarashid, "Communication overhead reduction in federated learning: A review," *Int. J. Data Sci. Anal.*, vol. 19, no. 2, pp. 185-216, Mar. 2025. (https://doi.org/10.1007/s41060-024-00691-x)

[19] J. F. Nash, "The bargaining problem," *Econometrica*, vol. 18, no. 2, pp. 155-162, Apr. 1950. (https://doi.org/10.1515/9781400829156-007)

[20] H. Park and M. van der Schaar, "Bargaining strategies for networked multimedia resource management," *IEEE Trans. Signal Process.*, vol. 55, no. 7, pp. 3496-3511, Jul. 2007. (https://doi.org/10.1109/TSP.2007.893755)

[21] A. E. Roth, *Game-theoretic models of bargaining*, Cambridge Univ. Press, 1985.

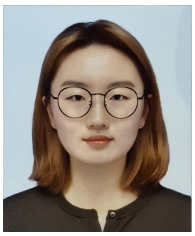
[22] N. Jin and E. Tsang, "Co-adaptive strategies for sequential bargaining problems with discount factors and outside options," in *Proc. IEEE Int. Conf. Evolutionary Computation*, pp. 2149-2156, Vancouver, BC, Canada, Jul. 2006. (https://doi.org/10.1109/CEC.2006.1688572)

[23] H. Xiao, K. Rasul, and R. Vollgraf, "Fashion-MNIST: A novel image dataset for benchmarking machine learning algorithms," *arXiv preprint arXiv:1708.07747,* 2017. (https://doi.org/10.48550/arXiv.1708.07747)

[24] Y. Lecun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," in *Proc. IEEE*, vol. 86, no. 11, pp. 2278-2324, Nov. 1998. (https://doi.org/10.1109/5.726791)

[25] J. Choi and H. Park, "Direction vector-based algorithm for the Nash bargaining solution in dynamic networks," *IEEE Commun. Lett.*, vol. 22, no. 7, pp. 1342-1345, Jul. 2018. (https://doi.org/10.1109/LCOMM.2018.2819644)

진 수 연 (Suyeon Jin)



2025년 2월 : 이화여자대학교 전자전기공학과 학사

2025년 3월~현재 : 이화여자대학교 전자전기공학과 석사과정

<관심분야> 게임이론, 인공지능, 머신러닝

[ORCID:0009-0004-5274-5503]

차 채 연 (Chaeyeon Cha)

2021년 2월 : 이화여자대학교 전자공학과 학사

2021년 3월~현재 : 이화여자대학교 전자전기공학과 석박사 통합과정

<관심분야> 게임이론, 최적화, 인공지능, 머신러닝

[ORCID:0000-0002-9027-9740]

박 형 곤 (Hyunggon Park)

2004년 2월 : 포항공과대학교 전자전기공학과 학사

2006년 3월 : University of California, Los Angeles (UCLA) M.S.

2008년 12월 : University of California, Los Angeles (UCLA) Ph.D.

2010년~현재 : 이화여자대학교 전자전기공학과 교수

<관심분야> 멀티에이전트 시스템 최적화, 머신러닝, 인공지능, 게임이론

[ORCID:0000-0002-5079-1504]